## IN THE CLAIMS

Please amend the claims as indicated:

1. (previously presented) A method of enabling use of a secure password, comprising:

during power up initialization before an operating system is started, copying security data from an unsecure memory device in a computer to a restricted portion of the computer's system memory which is invisible to the operating system, wherein the restricted portion of the computer's system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the computer's system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the computer's system memory, wherein the trusted software entity is a trusted routine that is part of a Basic Input/Output System (BIOS) Power-On Self Test (POST) program that is stored in the computer; and

before starting the operating system, hard locking the memory device against direct access so that a reset signal is required to unlock the memory device.

2. (original) The method of claim 1, further comprising:

responsive to receiving an entered password under the operating system, calling a routine executing within the restricted portion of system memory to verify the password; and

receiving an indication from the routine regarding whether the entered password matched a password within the security data copied to the restricted portion of system memory from the memory device.

3. (previously presented) The method of claim 1, wherein the step of copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system further comprises:

checking a return address for a call requesting that the security data be copied to verify that the call originated with the trusted routine.

4. (previously presented) The method of claim 3, wherein the step of checking a return address for a call requesting that the security data be copied to verify that the call originated with the trusted routine further comprises:

placing a label within a basic input/output services routine implementing a process for copying the security data immediately after instructions for the call requesting that the security data be copied;

placing an address for the label within code executing within the restricted portion of system memory and checking the return address for the call requesting that the security data be copied;

comparing the return address and the address for the label;

responsive to determining that the return address does not match the address for the label, returning a null response to the call requesting that the security data be copied; and

responsive to determining that the return address matches the address for the label, copying the security data to the restricted portion of system memory and resetting a retry counter.

5. (original) The method of claim 1, wherein the step of copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system further comprises:

copying the password and other sensitive data which requires protection from access under the operating system.

6. (original) The method of claim 1, wherein the step of copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system further comprises:

loading the security data to regular system memory prior to initiating the call requesting that the security data be copied; and

upon receiving any response to the call requesting that the security data be copied, erasing the security data from regular system memory before starting the operating system.

7. (previously presented) A method of enabling use of a secure password, comprising:

responsive to receiving an entered password under an operating system, calling a routine executing within a restricted portion of system memory to verify the password, wherein the restricted portion of system memory is invisible to the operating system and wherein the operating system and routines executing within the restricted portion of system memory communicate through a calling convention, and wherein the restricted portion of the system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the system memory, wherein the trusted software entity is a trusted routine in a Basic Input/Output System (BIOS) Power-On Self Test (POST) program that is stored in the computer; and

receiving only an indication from the routine executing within the restricted portion of memory regarding whether the entered password matched a password stored within the restricted portion of system memory.

8. (original) The method of claim 7, further comprising:

during power up initialization before the operating system is started, copying a password from a memory device to the restricted portion of system memory; and

before starting the operating system, hard locking the memory device against direct access so that a reset signal is required to unlock the memory device.

9. (original) The method of claim 7, further comprising:

determining whether a password is required for an operation by checking with the routine executing within a restricted portion of system memory to verify existence of a password.

10. (original) The method of claim 7, further comprising:

limiting a number of retries for a user to reenter a password.

11. (original) The method of claim 7, further comprising:

transmitting the entered password entered by a user to the routine executing within a restricted portion of system memory using the calling convention; and

responsive to receiving an indication from the routine executing within the restricted portion of memory that the entered password matched the password stored within the restricted portion of system memory, continuing an operation requiring the entered password for execution.

12. (previously presented) A data processing system, comprising:

a memory device which may be hard locked against direct access so that a reset signal is required to unlock the memory device; and

a power up initialization routine executing within the data processing system, wherein the power up initialization routine, before starting an operating system, copies security data from the memory device in a computer to a restricted portion of the computer's system memory which is invisible to the operating system and hard locks the computer's memory device, wherein the restricted portion of the computer's system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the computer's system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the computer's system memory.

13. (original) The data processing system of claim 12, wherein the power up initialization routine, responsive to receiving an entered password under the operating system, calls a routine executing within the restricted portion of system memory to verify the password and receives an indication from the routine regarding whether the entered password matched a password within the security data copied to the restricted portion of system memory from the memory device.

14. (original) The data processing system of claim 13, wherein the routine executing within the restricted portion of system memory checks a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine.

15. (original) The data processing system of claim 13, wherein the power up initialization routine, to facilitate checking a return address for a call requesting that the security data be

copied to verify that the call originated with a trusted routine, places a label within a basic input/output services routine implementing a process for copying the security data immediately after instructions for the call requesting that the security data be copied, wherein the routine executing within the restricted portion of system memory contains an address for the label, checks the return address for the call requesting that the security data be copied, and compares the return address and the address for the label and, responsive to determining that the return address does not match the address for the label, returning a null response to the call requesting that the security data be copied, and responsive to determining that the return address matches the address for the label, copying the security data to the restricted portion of system memory and resetting a retry counter.

16. (original) The data processing system of claim 12, wherein the power up initialization routine copies the password and other sensitive data which requires protection from access under the operating system.

17. (original) The data processing system of claim 12, wherein the power up initialization routine loads the security data to regular system memory prior to initiating the call requesting that the security data be copied and, upon receiving any response to the call requesting that the security data be copied, erases the security data from regular system memory before starting the operating system.

18. (previously presented) A data processing system, comprising:

an operating system;

a memory device which may be hard locked against direct access so that a reset signal is required to unlock the memory device;

a system memory including a restricted portion invisible to the operating system, wherein the operating system and routines executing within the restricted portion of system memory communicate through a calling convention; and

a power up initialization routine executing within the data processing system, wherein the power up initialization routine, responsive to receiving an entered password under an operating system, calls a routine executing within a restricted portion of system memory to verify the

password, and receives [[only]] an indication from the routine executing within the restricted portion of memory regarding whether the entered password matched a password stored within the restricted portion of system memory, wherein the restricted portion of the system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the system memory.

19. (original) The data processing system of claim 18, wherein the power up initialization routine, during power up initialization before the operating system is started, copies a password from the memory device to the restricted portion of system memory and, before starting the operating system, hard locks the memory device against direct access so that a reset signal is required to unlock the memory device.

20. (original) The data processing system of claim 18, wherein the power up initialization routine determines whether a password is required for an operation by checking with the routine executing within a restricted portion of system memory to verify existence of a password.

21. (original) The data processing system of claim 18, wherein the routine executing within a restricted portion of system memory to verify the password limits a number of retries for a user to reenter a password.

22. (original) The data processing system of claim 18, wherein the power up initialization routine transmits the entered password entered by a user to the routine executing within a restricted portion of system memory using the calling convention and, responsive to receiving an indication from the routine executing within the restricted portion of memory that the entered password matched the password stored within the restricted portion of system memory, continues an operation requiring the entered password for execution.

23. (previously presented) A computer program product within a computer usable medium for enabling use of a secure password, comprising:

instructions for copying security data from a memory device in a computer to a restricted portion of the computer's system memory which is invisible to the operating system during power up initialization before an operating system is started, wherein the restricted portion of the computer's system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the computer's system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the computer's system memory; and

instructions for hard locking the memory device against direct access so that a reset signal is required to unlock the memory device before starting the operating system.

24. (original) The computer program product of claim 23, further comprising:

instructions, responsive to receiving an entered password under the operating system, for calling a routine executing within the restricted portion of system memory to verify the password; and

instructions for receiving an indication from the routine regarding whether the entered password matches a password within the security data copied to the restricted portion of system memory from the memory device.

25. (original) The computer program product of claim 23, wherein the instructions for copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system further comprise:

instructions for checking a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine.

26. (original) The computer program product of claim 25, wherein the instructions for checking a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine further comprise:

instructions for placing a label within a basic input/output services routine implementing a process for copying the security data immediately after instructions for the call requesting that the security data be copied;

an address for the label within code executing within the restricted portion of system memory and checking the return address for the call requesting that the security data be copied;

instructions for comparing the return address and the address for the label;

instructions, responsive to determining that the return address does not match the address for the-label, for returning a null response to the call requesting that the security data be copied; and

instructions, responsive to determining that the return address matches the address for the label, for copying the security data to. the restricted portion of system memory and resetting a retry counter.

27-29. (cancelled)

30. (currently amended) The computer program product of claim [[29]] 23, wherein the restricted portion of the system memory is a System Management Interrupt (SMI) memory space.

31. (previously presented) The method of claim 1, wherein the restricted portion of the system memory is a System Management Interrupt (SMI) memory space.

32. (previously presented) The method of claim 7, wherein the restricted portion of the system memory is a System Management Interrupt (SMI) memory space.

33. (previously presented) The data processing system of claim 12, wherein the restricted portion of the system memory is a System Management Interrupt (SMI) memory space.

34. (previously presented) A method comprising:

asserting a Power-On Self Test (POST) Basic Input/Output System (BIOS) program in a computer;

in response to the POST BIOS program being asserted, setting a hard lock state on a non-volatile memory that contains sensitive data;

in response to the POST BIOS program being asserted, permitting an execution of a reading of the sensitive data in the non-volatile memory;

loading the sensitive data from the non-volatile memory into a non-protected system memory in the computer; and

in response to a call to code in a System Memory Interrupt (SMI) memory space, using the code in the SMI memory space to move the sensitive data from the non-protected system memory to the SMI memory space.

35. (previously presented) The method of claim 34, wherein the move of sensitive data from the non-protected system to the SMI memory space is permitted only if the call is a first request to copy the sensitive data from the non-protected system memory to the SMI memory space.

36. (previously presented) The method of claim 34, further comprising:

appending a label to a source code in the BIOS POST program, wherein the source code calls the code in the SMI memory space, and wherein the label contains an address of the source code;

checking on a stack a return address for the source code when the source code calls the code in the SMI memory space;

comparing the return address on the stack with the address in the label for the source code; and

storing the sensitive data from the non-protected system memory to the SMI memory space only in response to determining that the address on the stack is the same as the address in the label for the source code.